IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	: 10/786,224	Confirmation No.	: 2832
First Named Inventor	: Burkhard KUHLS		
Filed	: February 26, 2004		
TC/A.U.	: 2436		
Examiner	: Carlton Johnson		
Docket No.	: 080437.53236US		
Title	: Method for Providing Software to Be Used by a Control Unit of a Vehicle		

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On January 10, 2011, Appellants appealed to the Board of Patent Appeals from the final rejection of claims 1, 3-9 and 12-20. The following is Appellants' Appeal Brief submitted pursuant to 37 C.F.R. § 41.37. **An extension of the deadline for response to the Office Action is respectfully requested pursuant to 37 C.F.R. § 1.136(a) and the appropriate fee is submitted herewith.**

I. REAL PARTY IN INTEREST

An assignment of the present application to Bayerische Motoren Werke Aktiengesellschaft was recorded on July 19, 2004 at Reel/Frame 015547/0980.

II. RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any appeals, interferences or other proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 3-9 and 12-20 remain pending and are the subject of this appeal. Claims 2, 10 and 11 have been cancelled, and are not the subject of this appeal.

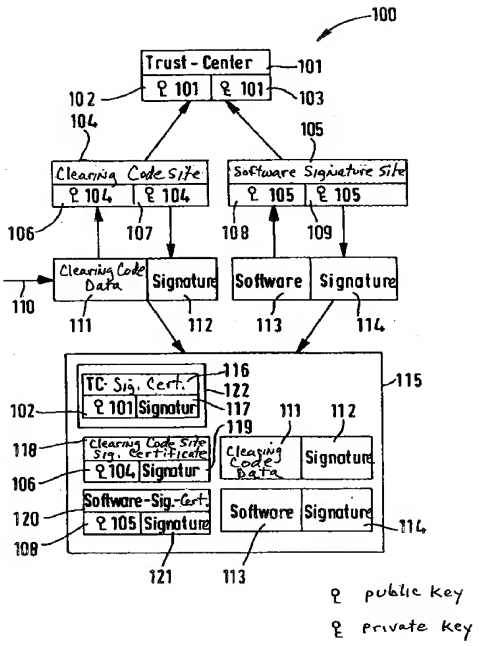
IV. STATUS OF AMENDMENTS

Appellant has not submitted any amendments after the final Office Action issued on September 29, 2010.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant discloses and claims novel and inventive methods for providing software for use by control units of a vehicle. Motor vehicles typically have control units operating using software. One problem that arises is that after the control unit is mounted in a vehicle the software may be exchanged or altered. This can be particularly problematic for control units that operate, among other things, vehicle safety systems.

Exemplary embodiments of the present invention address this and other problems of conventional systems by employing a variety of signatures, keys and certificates. In particular, referring to the sole figure (reproduced on the right), exemplary embodiments involve a trust center 101, software signature site 105, clearing code site 106 and control unit 115. The control unit 115 can store the following certificates[1]:



1. A trust center certificate 116 generated using secret key 103 of trust center 101 and including public key 101 and signature 117 generated using secret key 103;

2. A clearing code site signature certificate 118 generated using public key 106 of clearing code site 104 and private key 103 of trust center 101;

3. A software signature certificate 120 generated using private key 103 of trust center 101 and public key 108 of software signature site 105, and including public key 108 of software signature site 105, a signature 121 generated by trust center 101 and one or more validity restrictions.

[1] Figure 1 and page 7, lines 19-20; paragraph 0026.

Control unit 115 can also store clearing code data 111 with an associated signature 112, and software 113 and an associated signature 114.[2] These signatures, keys and certificates provide a particularly advantageous technique for ensuring that software executed by a control unit is actually authorized for such execution.

Turning now to the claims, claim 1 recites a method of providing software 113 for use by a control unit 115 of a vehicle. A software signature certificate 120 is generated using the public key 108 of the software signature site 103 and a secret key 103 of a control entity of a trust center 101, according to a public-key method.[3] A signing and two checking acts are executed prior to execution of the software by the control unit. Specifically, the software is signed against falsification using a secret or private key 109 of a software signature site 105, according to a public-key method.[4] The software signature certificate 120 is checked for integrity according to a public-key method using a public key 102 of the trust center 101.[5] The signed software 113, 114 is checked for integrity using a public key 108 of the software signature site 105 contained in the software signature certificate 120, the public key 108 of the software signature site 105 being complementary to the secret key 109 of the software signature site 105.[6]

Claim 7 recites a method of providing software 113 for use by a control unit 115 of a vehicle. Before its use by the control unit, the software 113 is signed against falsification using a secret or private key 109 of a software signature site 105 according to a public-key method.[7] The signed software 113, 114 is checked for integrity using a public key 108 complementary to the secret key 109 of the software signature site 105. The control unit 115

[2] Figure 1.
[3] Page 6, lines 9-11; paragraph 0022.
[4] Page 7, lines 14-18; paragraph 0025.
[5] Page 8, lines 15-19; paragraph 0028.
[6] Page 9, lines 3-8; paragraph 0029.
[7] Page 7, lines 14-18; paragraph 0025.

stores a clearing code site signature certificate 118, a software signature certificate 120, clearing code data 111 and their signature 112 as well as the software 113 and its signature 114.[8] The software signature certificate 120 is generated using the public key 108 of the software signature site 105 and a secret key 103 of a control entity of a trust center 101.[9]

Claim 19 recites a method of providing software 113 for use by a control unit 115 of a vehicle. The control unit 115 stores a software signature certificate 120 and receives signed software 113, 114.[10] The control unit 115 checks whether the software signature certificate 120 has been changed or manipulated and whether the signed software 113, 114 has been changed or manipulated.[11]

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The one ground of rejection for review on appeal is the rejection of claims 1, 3-9 and 12-20 for obviousness under 35 U.S.C. § 103(a) as being obvious in view of the combination of England et al. (US 6,330,670, hereinafter "England"), Ishii (US 5,768,389) and Wong et al. (US 5,957,985, hereinafter "Wong").

VII. ARGUMENT

A. Brief Summary of the Prosecution History

Almost four years ago substantive examination began with the issuance of a non-final rejection on June 1, 2007. Since that time prosecution has involved:

- Three additional non-final Office Actions;
- Four final Office Actions;
- Three Advisory Actions; and
- Two Pre-Appeal Brief Conference Requests that resulted in reopening of the prosecution.

[8] Page 9, lines 3-8; paragraph 0029.
[9] Page 6, lines 9-11; paragraph 0022.
[10] Figure 1 and page 7, lines 19-20; paragraph 0026.
[11] Page 8, lines 15-19 and page 9, lines 3-8.

Despite the issuance of eleven communications related to substantive examination by the Patent Office, Appellant has not filed a Request for Continued Examination (RCE). The Wong patent that is part of the current rejection was included in the rejection in the first Office Action, and the England patent was added when prosecution was reopened in response to Appellant's first Pre-Appeal Brief Conference Request.

The reversible error that is present in the current rejection was first introduced in the Advisory Action mailed on February 2, 2009. In particular, as discussed in the second Pre-Appeal Brief Conference Request, the Advisory Action appeared to base the rejection on what the Examiner considered to be the "gist" of the invention instead of considering the actual claim language. This improper reasoning has evolved such that the current rejection appears to be based on the position that because the basic concepts of certificates, keys and signatures are known, the particular types of certificates, keys and signatures recited in the claims is irrelevant to the conclusion of obviousness. This reasoning, however, goes against the established law that "All words in a claim must be considered in judging the patentability of that claim against the prior art."[12] As such, the rejection of Appellant's claims is based upon reasoning that is clearly reversible error.

B. The Combination of England, Ishii and Wong Does Not Render Claim 1 Obvious

Appellant does not dispute that both England and Ishii disclose cryptography techniques employing public and private keys, England discloses signing certificates, and Ishii discloses signing keys as a certification.[13] The points of disagreement are whether:

- Ishii's disclosure of signing a key is performed in the same manner as the generation of a software signature certificate in claim 1;

[12] M.P.E.P. § 2143.03, quoting *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

[13] Wong is cited solely for the disclosure of a vehicle control unit but does not otherwise remedy the deficiencies of the combination of England and Ishii. Accordingly, Wong will not be addressed any further in this Brief.

- England's processing of the ***CPU*** certificate operates in the same manner as the checking of the ***software*** signature certificate for integrity in claim 1; and
- England's checking of a ***CPU*** certificate for integrity is the same as checking signed ***software*** for integrity.

As will become apparent in the discussion below, these disclosures of England and Ishii do not disclose or suggest the generation of a software signature certificate or checking a software signature certificate and signed software in the manner recited in claim 1.

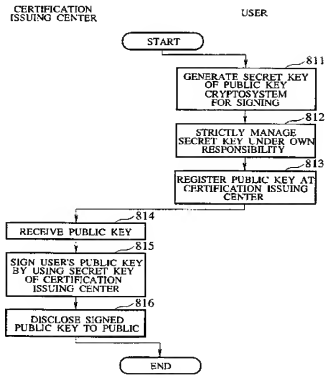
1. The Combination of England, Ishii and Wong Does not Disclose or Suggest Generating a Software Signature Certificate in the Manner Required by Claim 1

Claim 1 does not simply recite that a software signature certificate is generated, but instead requires that the certificate is generated in a particular manner using particular keys. Specifically, claim 1 recites:

> generating a software signature certificate using the public key of the software signature site and a secret key of a control entity of a trust center, according to a public-key method,

The Examiner recognizes that England does not disclose generating a software signature certificate in this manner, and instead cites to column 5, lines 43-67 of Ishii. The cited section of Ishii is part of the Summary of the Invention section, which corresponds to the sixth embodiment discussed in connection with FIGs. 22 and 23 of the Detailed Description section. As illustrated in FIG. 22 of Ishii (reproduced on the right), a user's public key is signed using a secret key of the certification issuing center (step 815) and the "signed public key is disclosed to the public as this user's certification (step 816)."[14]

FIG.22



In contrast to the requirement of Appellant's claim 1 of generating the certificate "using the public key of the ***software signature site***"[15], Ishii discloses the use of "a ***user's***

[14] Column 31, lines 12-13.

public key"[16]. Thus, even if it were assumed that the result of the signing in step 815 of Ishii was a software signature certificate, it would be generated using "a ***user's*** public key"[17] and not "the public key of the ***software signature site***"[18] as required by Appellants' claim 1.

Instead of directly addressing Appellant's arguments, for example by identifying the flaws in the arguments, the Advisory Action merely repeats the same statement from the Response to Arguments section of the final Office Action, which statement actually highlights that the rejection is based upon a distillation of the claim and not the actual claim language:

> Ishii discloses the generation of a signature (a standard cryptographic processing function) using a public key of one entity and a secret key of another entity. (Ishii col 5, lines 43-67; signing (signature certificate) by using the secret key of certification issuing center (first public key cryptosystem); deciphering processing using the secret key or encryption processing (signature generation) using the public key or the second public key cryptosystem; cryptographic processing (signature generating using a public key and a secret key)[19]

Appellant's claim 1 does not simply recite generating a signature using public and private keys of two generic entities (i.e., first and second public key cryptosystems), but instead specifies that the public key is of a ***software signature site*** and the secret key is of a ***control entity of a trust center***. Thus, a generic disclosure of "using a public key of one entity" does not render obvious the claim requirement of "using the public key of the ***software signature site***". Additionally, the Advisory Action does not explain why Ishii's "first public key cryptosystem" is the control entity of a trust center as recited in claim 1 or why Ishii's "second cryptosystem" is the software signature site recited in claim 1.

---

[15] Emphasis added.
[16] Emphasis added.
[17] Emphasis added.
[18] Emphasis added.
[19] Page 5.

Moreover, even if the statement above were accepted as an accurate characterization of the application of Ishii to Appellant's claim 1, which it is not, it still does not completely address how Ishii discloses or suggests generating a software signature certificate in the same manner as claim 1. Instead of addressing the use of a public ***and*** private key to generate a certificate, the statement above appears to only assert that a secret key is used to generate the certificate and that the public key is only used for "deciphering processing". Thus, accepting the statement above as accurate would still result in generating a certificate using only a secret key, but not both a public and secret key, much less the specific public and secret keys recited in claim 1.

Because Ishii's disclosure of a ***user's*** public key is not the same as the claim requirement of "using the public key of the ***software signature site***"[20], Ishii does not disclose or suggest generating a software signature certificate in the same manner as required by the language of claim 1. England and Wong do not remedy these deficiencies of Ishii, and accordingly even if one skilled in the art were motivated to combine England, Ishii and Wong, the combination would not disclose or suggest this claim element.

Finally, it is noted that the discussion in the Advisory Action begins with the statement that the "software signature site (a software program, module) acting as a user can be associated with the owner of the public/private key pair."[21] The Advisory Action provides no prior art citation or any further reasoning to support this statement. As such, there is no evidence in the record to support this position, and accordingly the statement should be disregarded as nothing more than unsubstantiated opinion.

[20] Emphasis added.
[21] Page 2.

2. The Combination of England, Ishii and Wong Does not Disclose or Suggest Checking a Software Signature Certificate in the Manner Required by Claim 1

Claim 1 does not just recite checking a software signature certificate, but instead requires that this check is performed using a particular key:

> checking the software signature certificate for integrity according to a public-key method using a public key of the trust center; and

The rejection relies upon England's CPU certificate and checking signed software as corresponding to this claim element, an interpretation of England that is not supported by the actual disclosure of England. Specifically, to reject this element set forth above the Office Action states:

> see England col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 8, line 66 – col.9, line 3: trusted third party (use digital signature for authentication); trusted third party equivalent to trust center)[22]

Column 8, lines 7-14 of England discusses a certificate that is created for a CPU. The CPU certificate of England is relates to a CPU and not to software, and accordingly the CPU certificate is not the same as the claimed "software signature certificate".

Regarding the signing of software, as can be seen by reviewing column 8, line 66-column 9, lines 3 of England (reproduced below), the section of England cited in the rejection generically discusses signing software but does not disclose or suggest that a software signature certificate is signed or that such a certificate is signed using a public key, much less a public key of a trust center.

> The first requirement is met in the exemplary embodiment of the invention by having ***all trusted operating system-level components digitally signed*** by their developers

[22] Page 8.

> or a trusted third-party, with the signature acting as a guarantee that the components respect digital rights.[23]

As such, this generic disclosure of signing operating system-level components does not disclose or suggest the specific requirement of claim 1 that a software signature certificate is signed using a public key of a trust center.

The Office Action does not explain how England's disclosure of signing trusted operating system-level components relates to the claim recitation of "checking the software signature certificate". Accordingly, Appellant previously attempted to address this citation to England by explaining that England does not disclose or suggest that a software signature certificate is an operating system-level component. Contrary to the discussion in the Response to Arguments section of the final Office Action[24], Appellant was not arguing that the claimed software signature certificate is an operating system component. Quite the opposite, Appellants' were arguing that England's disclosure of signing operating system-level components has no disclosed relationship to the claimed software signature certificate.

Additionally, the discussion in the Response to Arguments section of the final Office Action addressing the checking of the software signature certificate again demonstrates that the rejection is not based on the claim language itself, but instead on the idea that generic disclosures of keys and certificates renders obvious the particular keys and certificates recited in claim 1:

> England also discloses utilizing certificates with public and private key pairs with certificates to verify a digital signature.
>
> In addition, England does disclose checking a signature certificate for integrity.
>
> For additional clarity, England discloses a certificate is signed, therefore the certificate can be checked for validity by

[23] Emphasis added.
[24] Page 2.

> checking its digital signature. (see England, col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)[25]

The first two sentences merely state what is asserted to be disclosed by England without any citation of support. As such, these first two sentences do not provide any evidence to support the rejection. The remainder of this discussion confuses England's disclosure of a signed CPU certificate with the verification of operating system-level components. Again, England does not disclose or suggest that a ***CPU certificate*** is a ***software signature certificate***. Additionally, England's disclosure in column 11, lines 54-59 of checking the signature of operating level-system components does not have any relation to checking the CPU certificate discussed in column 8, lines 7-14.

Because there is no evidence in the record that England's CPU certificate is a software signature certificate and the rejection has not cited any other certificate in England, the rejection has provided no evidence that England discloses or suggests "checking the software signature certificate" in the manner recited in claim 1.

In response to these arguments the Advisory Action addresses the signing of the software and the checking of the signed software signature certificate for integrity in a combined fashion, making it difficult to identify the arguments directed to each of these separately recited claim elements. It is unclear why the Examiner has addressed these two claim elements together, particularly considering that the claim clearly distinguishes between signed software and a software signature certificate; and the software is signed using the key of a software signature site, whereas the software signature certificate is checked using a public key of the trust center. In order to appreciate these issues, the discussion in the Advisory Action is reproduced below:

---

[25] Page 3.

> 2. The claim limitation states: "signing the software against falsification" and "checking the signed software signature site certificate for integrity" (Claim 1).
>
> This limitation discloses that the software is signed. England discloses that software is signed. (see England col. 11, lines 47-51; boot block and all loaded components signed by a trusted source and provide with a certificate; col. 11, lines 54-59: checks digital signature of a component before loading it; signature valid then component has not been compromised and loaded) And, the certificate for the software signature site is signed and the site signature attached to the certificate is checked for integrity (determined tampering). (see England col. 8, lines 7-14: certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 8, lines 66-col. 9, line 3: trust third party (use digital signature for authentication); trusted third party equivalent to trust center)
>
> The manufacture of the software (based on specification) is the software signature site. England discloses a manufacturer of the software (OS software). This disclosure appears to be equivalent to the claimed invention. The manufacturer of the software is also the manufacturer of the CPU. This fact of manufacturing the CPU does not negate from the fact that the indicated manufacturer is also the manufacturer of the software which is signed and checked for integrity. The manufacture of the software signs the software and the manufacturer of the software signs the certificate (public/private keys).[26]

By interpreting signing the software and checking the integrity of the certificate as the same claim limitation, the Examiner ignores the plain language of the claim that these are separately recited elements and also improperly relies upon England's disclosure of checking the ***signed software*** for integrity as the same as checking a software ***signature certificate*** for integrity. Checking signed software is not the same as checking a certificate for integrity, and the Examiner has provided no argument or reasoning as to why these are the same.

Additionally, the argument in the third paragraph reproduced above that the CPU and OS manufacturer are the same is unsupported by any evidence, and indeed appears to be contradicted by England. Notably absent is any citation to England supporting the position

[26] Page 2.

that the CPU and OS are from the same manufacturer. Additionally, England specification mentions both a CPU manufacturer[27] and an operating system vendor[28], thereby implying that they are different. England does not discuss that the CPU manufacturer and operating system vendor are the same, as asserted in the Advisory Action. Indeed, the assignee on the face of England is Microsoft, a company that is an operating system vendor, but not a CPU manufacturer. As such, the arguments provided in the Advisory Action do not support the Examiner's position that England's disclosure of checking a CPU certificate is the same as checking a software signature certificate, much less that it is performed in the same manner as recited in claim 1. Ishii and Wong do not remedy this deficiency of England, and accordingly even if one skilled in the art were motivated to combine England, Ishii and Wong, the combination would not disclose or suggest this claim element.

3. The Combination of England, Ishii and Wong Does not Disclose or Suggest Checking Signed Software for Integrity in the Manner Required by Claim 1

Appellant's claim 1 does not simply recite that the signed software is checked for integrity, but instead recites a particular technique for doing so. Specifically, the claim recites:

> checking the signed software for integrity, using a public key of the software signature site contained in the software signature certificate, the public key of the software signature site being complementary to the secret key of the software signature site.

To reject this claim element the Office Action states:

> (see England col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate; col. 11, lines 54-59: checks digital signature of a component before lading it; signature valid then component has not been compromised and loaded)

[27] See, for example, column 7, line 51.
[28] See, for example, column 13, lines 14-15.

> The digital rights OS components are loaded and the digital signature is checked for each component before loading. And, England discloses a signed digital certificate from the manufacturer of the control unit (CPU) and OS software.
>
> This is equivalent to disclosure in the specification on page 6, paragraph [0021], lines 3-6, that discloses a software signature certificate is generated and signed by the manufacturer of the software.[29]

Column 11, lines 47-59 of England discuses that the signature of software components are checked before they are allowed to be loaded. It does not specify how this check is performed. Indeed, it does not disclose or suggest that this is performed "a public key of the software signature site contained in the software signature certificate" as recited in claim 1.

The citation to the ***CPU certificate*** has no apparent relevance to the claim recitation of checking the ***signed software*** for integrity using a public key ***contained in the software signature certificate*** because the CPU certificate is for the CPU and not for software. Additionally, the disclosure on page 6 of Appellants' specification does not indicate an equivalence between a CPU certificate and a software signature certificate as asserted in the Office Action.

Although column 11, lines 50-53 of England discloses that all components are signed and "provided with a rights manager certificate", there is no disclosure or suggestion that this certificate includes a public key of a software signature site that is used for checking the integrity of signed software. The rights manger certificate is disclosed in FIG. 9 of England (reproduced below).

[29] Page 8.

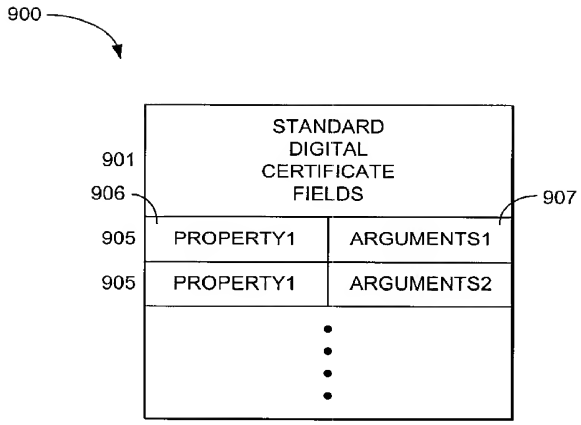


Fig. 9

England describes the certificate as including information related to digital rights management but is silent with respect to the certificate including a public key of a software signature site as recited in Appellants' claim 1:

> A list of application properties 903 is appended to the digital certificate fields 901 standard in some digital certificate format such as X.509. The certificate names the application. Each entry 905 in the list 903 defines a property 906 of the application, along with optional arguments 907. For example, one property might be that the application cannot be used to copy content. Another example of a property is one that specifies that the application can be used to copy content, but only in analog form at 480P resolution. Yet another example of a property is one that specifies that the application can be used to copy content, but only if explicitly allowed by an accompanying license. Additional examples include the right to store an encrypted copy of the content and to restrict such storage to only certain, acceptable peripheral devices. The property 906 can also be used to specify acceptable helper applications, such as third-party multimedia processing stacks or other libraries, to be used in conjunction with the application named in the certificate.

Accordingly, there is no disclosure or suggestion in England that the digital rights management certificate includes a public key of a software signature site that is used to check the integrity of signed software as recited in claim 1.

The Response to Arguments section of the Office Action does not provide any evidence that England discloses checking the integrity of the signed software in the particular manner recited in claim 1, but instead that England discloses generically checking the integrity of signed software. Specifically, the Office Action states:

> England discloses that the signature of the boot block is checked before loading the digital rights OS. The software is checked for integrity before its usage as a digital rights OS. (see England col 9, lines 7-10: digital rights OS; col 8, 48-51: system incorporates public/private key pairs, digital certificates; col. 8, lines 34-37: boot block signed by OS manufacturer; (boot block processed before execution or use of software); col. 11, lines 47-51: boot block and all loaded components signed by a trusted source and provided with a certificate)
>
> In addition, England does disclose checking a signature certificate for integrity.
>
> For additional clarity, England discloses a certificate is signed, therefore the certificate can be checked for validity by checking its digital signature. (see England, col. 8, lines 7-14; certificate is signed and signature checked for validity of certificate, public/private key pair usage; col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised)[30]

The first paragraph reproduced above does not address how England discloses that the software is checked for integrity using a public key contained in a software signature certificate. The second paragraph is not provided with any supporting citation to England, and thus provides no evidence that England discloses that the software is checked for integrity using a public key contained in a software signature certificate. As discussed above, the third paragraph confuses England's disclosure of a signed CPU certificate with the verification of operating system-level components. It does not provide any evidence that the software is checked for integrity using a public key contained in a software signature certificate. Thus, there is no evidence supporting the position that England discloses or

[30] Pages 2 and 3.

suggests the checking of the signed software for integrity in the same manner as that recited in Appellant's claim 1.

Ishii and Wong do not remedy this deficiency of England, and accordingly even if one skilled in the art were motivated to combine England, Ishii and Wong, the combination would not disclose or suggest this claim element.

C. The Combination of England, Ishii and Wong Does Not Render Claim 7 Obvious

The combination of England, Ishii and Wong does not render claim 7 obvious because the combination does not disclose or suggest a control unit storing:

1. a clearing code site signature certificate,
2. a software signature certificate,
3. clearing code data and their signature; and
4. software and its signature.

Specifically, the cited section of England[31] only mentions that a CPU can be equipped with a pair of public and private keys, but does not mention any certificates, clearing code data or clearing code data signature.

The Response to Arguments section responds to Appellants' argument by stating:

> England discloses a certificate (software signature, clearing code signature) which contains a public/private key pair for each particular certificate. England also discloses (see England col. 7, lines 50-54: storage of keys, certificates; manufacture equips the CPU with a pair of public and private keys that is unique to the CPU; certificate contains public key)
>
> England discloses the clearing code data (identity) and signature capability for a certification (clearing code certificate. (see England col. 8, lines 26-28; col. 9, lines 4-10; software identity; identify of an authenticated OS)[32]

[31] Column 7, lines 50-54.
[32] Pages 3 and 4.

It appears that the first sentence is attempting to equate certificates with signatures. England, however, clearly distinguishes between certificates and signatures. For example, England discusses signing certificates. If certificates were the same as signatures, then England would disclose applying a certificate to a certificate, which England does not.

The second paragraph appears to rely upon England's CPU certificate. It does not, however, describe which of the claimed certificates correspond to the CPU certificate. Regardless, England's CPU certificate does not correspond to any of the claimed certificates.

The third paragraph appears to assert that England discloses the claimed clearing code site signature certificate, however, the citations relates storage of the identity of an authenticated digital rights operating system in a CPU. There is no explanation of how storage of an operating system identity in a CPU relates to a clearing code signature site certificate as recited in claim 7.

The Advisory Action repeats the same argument reproduced above and adds an explanation following the second paragraph:

> This is equivalent to the specification on page 3, paragraphs [0010] and [0012], which discloses that the clearing code certificate contains an identifier and the capability to restrict usage to a particular control entity.

Thus, it appears that the rejection is based on the CPU certificate as corresponding to the claimed clearing code data and their signature. Even if it were assumed that this is correct, which it is not, then the rejection would be missing a disclosure of a software signature certificate because the rejection relies upon the CPU certificate for the disclosure of both the software signature certificate and the clearing code data. Claim 7 clearly distinguishes between the two, and accordingly a CPU certificate cannot disclose or suggest both the software signature certificate and the clearing code data and their signature.

This reasoning also fails to account for the language of claim 7, which recites the use of "clearing code data and their signature" and not a clearing code certificate as asserted in the Office Action.

Ishii and Wong do not remedy the above-identified deficiencies of England, and accordingly the combination cannot render claim 7 obvious.

D. The Combination of England, Ishii and Wong Does Not Render Claim 19 Obvious

Regarding claim 19, the combination of England, Ishii and Wong does not render this claim obvious because the combination does not disclose or suggest a control unit that checks whether a ***software signature certificate*** and signed software has been changed or manipulated.

As previously discussed, the Office Action's reliance on England's disclosure of checking software component signatures for validity does not disclose or suggest checking ***a software signature certificate*** for manipulation as required by claim 19.

The Response to Arguments section, however, does not address how England discloses checking the particular certificate recited in claim 19, i.e., the ***software signature certificate***. Instead, it highlights the Office Action's continued insistence on relying upon generic disclosures to reject the specifics of Appellants' claims. Specifically, the Office Action states that:

> A certificate (***no matter what type***) is still digital information and its integrity can be checked using digital signature verification procedures. England discloses the verification of ***whether digital information (a digital certificate***) has been modified or changed. (see England col. 11, lines 54-59: checks signature of a component before loading it; if signature valid then component has not been compromised) The Examiner is operating under the assumption that when a component is signed then the component is protected. Any modification or updates to the

> certificate can be discovered by checking the digital signature.[33]

Simply because England discloses checking the signature of software components, and software components and digital certificates are both digital data does not mean that England discloses or suggests checking the particular certificate recited in Appellants' claim 19, i.e., a ***software signature certificate***. Again, it appears that the rejection ignores the actual claim language in order to support the rejection and instead is based on a distillation of the claim language. This is clearly improper.

Additionally, the reasoning provided is not supportable. Although a certificate is digital information does not mean all digital information is a certificate. For example, a word processing document stored on a computer is digital information, but this does not mean one skilled in the art would interpret a word processing document as a certificate.

Moreover, this reasoning relies upon an inconsistent interpretation of England because it relies upon a signed operating system as corresponding to the claimed signed software, but also relies upon other types of signed software as corresponding to the claimed software signature certificate. One skilled in the art would either interpret a signed operating system and signed software both as signed software (which is the most likely possibility) or both as a software signature certificate. One skilled in the art would not interpret some signed software (e.g., the operating system) as signed software and other signed software (software components loaded by the operating system) as a software signature certificate.

Instead of addressing this argument, the Advisory Action merely repeats the same reasoning provided in the final Office Action. Thus, there is no evidence in the record that one skilled in the art would interpret all digital data as a certificate or that some signed software as signed software and other software as a certificate.

---

[33] Page 4 and 5. (Emphasis added).

Ishii and Wong do not remedy this deficiency of England, and accordingly the combination cannot render claim 19 obvious.

E. The Combination of England, Ishii and Wong Does Not Render Dependent Claims 3-6, 8, 9, 12-18 and 20 Obvious

These dependent claims are patentably distinguishable over the combination of England, Ishii and Wong at least by virtue of their dependency. Additionally, the rejection of these dependent claims also relies upon a distillation of the claims and not the actual language recited in the claims. Thus, for example, the rejection of claims 4 and 5 does not account for the particular manner of signing the clearing code data (claim 4) or the particular manner of generating the clearing code site certificate (claim 5).

Accordingly, the rejection of dependent claims 3-6, 8, 9, 12-18 and 20 for obviousness should be reversed.

VIII. CONCLUSION

For the foregoing reasons it is respectfully that the rejections of Appellant's claims 1, 3-9 and 12-20 are improper, and therefore, these grounds of rejection should be reversed.

The Appeal Brief is being submitted with the required fee of $540.00. This amount is believed to be correct, however, the Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, to Deposit Account No. 05-1323, Docket No. 080437.53236US.

Respectfully submitted,

March 17, 2011

/Stephen W. Palan, Reg. No. 43,420/
Stephen W. Palan
Registration No. 43,420

CROWELL & MORING LLP
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:crr
14305662

CLAIMS APPENDIX

1. A method of providing software for use by a control unit of a vehicle, said method comprising:

generating a software signature certificate using the public key of the software signature site and a secret key of a control entity of a trust center, according to a public-key method,

wherein prior to execution of the software by the control unit,

signing the software against falsification, using a secret or private key of a software signature site, according to a public-key method;

checking the software signature certificate for integrity according to a public-key method using a public key of the trust center; and

checking the signed software for integrity, using a public key of the software signature site contained in the software signature certificate, the public key of the software signature site being complementary to the secret key of the software signature site.

2. (Canceled)

3. The method according to Claim 1, wherein one of a control entity certificate and a trust center certificate is generated according to a public-key method by using the secret key of the control entity.

4. The method according to Claim 1, wherein clearing code data are signed using a secret key of a clearing code site according to a public key method.

5. The method according to Claim 1, wherein a clearing code site signature certificate is generated using the secret key of the control entity of the trust center according to a public-key method.

6. The method according to Claim 3, wherein the trust center certificate is protected against falsification and exchange, in a protected memory area in the control unit.

7. A method of providing software for use by a control unit of a vehicle, said method comprising:

before its use by the control unit, signing the software against falsification, using a secret or private key of a software signature site, according to a public-key method; and

checking the signed software for integrity, using a public key complementary to the secret key of the software signature site, wherein a clearing code site signature certificate, a software signature certificate, clearing code data and their signature as well as the software and its signature are stored in the control unit, and the software signature certificate is generated using the public key of the software signature site and a secret key of a control entity of a trust center.

8. The method according to Claim 1, wherein the software signature certificate includes at least one validity restriction.

9. The method according to Claim 5, wherein the clearing code site signature certificate includes at least one validity restriction, a restriction to a particular control unit

which is designated by means of an identification number stored in the control unit in an invariable manner, and a restriction to a vehicle identification number of a particular vehicle.

10. (Canceled)

11. (Canceled)

12. The method according to Claim 5, wherein the clearing code site signature certificate is checked for integrity according to a public key method, using a public key of the trust center.

13. The method according to Claim 4, wherein the signed clearing code data are checked for integrity according to a public key method, using a public key of the clearing code site contained in the clearing code site signature certificate.

14. The method according to Claim 1, wherein the control unit is equipped with a sequence-controlled microprocessor that implements one of the above-described methods.

15. A control unit for a motor vehicle, which implements a method according to Claim 1.

16. A data processing system for a motor vehicle, which implements a method according to Claim 1.

17. A computer program product sequence control of a data processing system of a motor vehicle or motorcycle, which implements the method according to Claim 1.

18. A data carrier, comprising a computer program product according to Claim 17.

19. A method of providing software for use by a control unit of a vehicle, said method comprising:

storing, by the control unit, a software signature certificate;

receiving, by the control unit, signed software;

checking, by the control unit, whether the software signature certificate has been changed or manipulated; and

checking, by the control unit, whether the signed software has been changed or manipulated.

20. The method of claim 19, further comprising:

storing, by the control unit, a trust center certificate that includes a public key and a signature generated using a secret key of a trust center; and

storing, by the control unit, a clearing code site signature certificate that includes a second public key and a second signature,

wherein the software signature certificate includes a third public key and a third signature.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.